



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

11/2

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/527,670	03/17/2000	Ghun-up Cha	0630-0983P	2822
7590	02/21/2006		EXAMINER	
Birch Stewart Kolasch & Birch LLP P O Box 747 Falls Church, VA 22040-0747				ARANI, TAGHI T
		ART UNIT		PAPER NUMBER
		2131		

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/527,670	CHA ET AL.	
	Examiner Taghi T. Arani	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 28 October 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 13-20,28,29,31-33,36,38 and 40-55 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 13-20 and 40-55 is/are rejected.

7) Claim(s) 28,29,31-33,36 and 38 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892) 4) Interview Summary (PTO-413)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948) Paper No(s)/Mail Date. ____ .
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date ____ . 5) Notice of Informal Patent Application (PTO-152)
6) Other: ____ .

DETAILED ACTION

1. Claims 13-20, 28-29, 31-33, 36, 38, and 40-55 have been examined and are pending

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.14. Applicant's submission filed on 10/28/2005 has been entered.

Response to Amendment

3. Applicant's amendment filed 10/28/2005 necessitated the new ground(s) of rejection presented in this Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 13-20 are rejected under 35 U.S.C. 102(e) as being anticipated by prior art of record, Wiser et al., U.S. Patent No. 6,330 (hereinafter “Wiser”).

As per claim 13, Wiser teaches a method for copy protection, comprising:

generating a partially decrypted data unit (col. 2, lines 20-28), the partially decrypted data unit including two portions, each one of the two portions is encrypted having a protection level different from the other of the two portions (col. 2, lines 28-41, see also col. 4, lines 47-63, i.e. the first encryption/decryption unit uses DES algorithm with a 56-bit key and the second encryption/decryption unit employs the RC4 algorithm using 40-bit key); and

transferring the partially decrypted data unit to a target device for further decrypting based on information used in the step of generating the partially decrypted data unit (col. 6, lines 15-24, i.e. Decryption engine 214 (target device) incrementally decrypts the intermediate file).

As per claim 14, Wiser teaches the method of claim 13, wherein the two portions having the different protection levels are spaced apart at a predetermined interval on the data unit (col. 5, lines 45-50).

As per claim 15, Wiser teaches the method of claim 14, further comprising the step of storing the partially decrypted data unit in a data storage medium or a digital data player (Fig. 2, LOCAL STORAGE MEDIUM 212, col. 6, lines 6-10, see also col. 5, lines 66-67).

As per claim 16, Wiser teaches the method of claim 14, further comprising the step of decrypting a remainder of the partially decrypted data unit in the target device (col. 5, lines 42-50).

As per claim 17, Wiser teaches the method of claim 13, wherein the data unit is partially decrypted based on a predetermined encryption key (col. 5, lines 35-38, i.e. according to 56-bit DES).

As per claim 18, Wiser teaches the method of claim 15, further comprising the step of reading the partially decrypted stored data unit from the data storage medium or the digital data

player and reproducing the data unit at the request of a user (col. 4, lines 2-14, see also col. 6 lines 15-24).

As per claim 19, Wiser teaches the method of claim 18, further comprising the step of decrypting the data unit based on a predetermined encryption key, and outputting the decrypted data unit to an output line (col. 6, lines 6-9, lines 16-24, write the decrypted portions to the CD-R medium (i.e. an output line)).

As per claim 20, Wiser teaches the method of claim 14, wherein the predetermined interval is a multiple or divisor of a buffer size (col. 5, lines 60, col. 6, lines 28-24).

5. Claims 13-20 are rejected under 35 U.S.C. 102(e) as being anticipated by prior art of record, Satio, U.S. Patent No. 5,867,579.

As per claims 40, 44, 48, 51, 54 and 55, Satio teaches a method for encrypting a digital data file, comprising (Abstract):

receiving a data file from a digital data server, the data file having been encrypted in the digital data server based on a predetermined encryption key (col. 5, lines 20-22);

decrypting the data file using the predetermined encryption key (col. 5, lines 40-46);

identifying whether or not the received data file needs to be protected (col. 5, lines 52-54, i.e. to store, copy or transfer the data M as the original data M0 or the edited data M1, it is encrypted);

reencrypting the decrypted data file on the basis of the identified result (col. 5, lines 55-61); and

transferring the reencrypted data file to a target device (col. 6, lines 10-17, i.e.

transferring encrypted Cmks2 to terminal 5, see also col. 33, lines 33-40), wherein the reencrypted data file has a different level of encryption as compared to that of the received data file that was encrypted in the digital data server (col. 4, line 58-61, the original data M0 is encrypted using Ks1 while reencryption is carried using Ks2, col. 5, lines 55-56, i.e. two different keys providing different level of encryption.

As per claim 44, Satio teaches the method of claim 40, wherein the step of generating the encrypted data unit is based on a predetermined encryption key (col. Col. 4, lines 33-35, i.e. Ks1, lines 58-61, and the data unit M0 is encrypted using Ks1).

As per claim 48, Satio teaches a method for copy protection, comprising the steps of: enabling a registration mode for inputting a user identification (col. 4, lines 14-32); receiving a data unit from a storage device based on the inputted user identification information (col. 4, lines 42-57), wherein the data unit has been encrypted (col. 4, lines 58-64); generating an encrypted data unit having a different encryption level or method from one used to encrypt the data unit (col. 5, lines 52-61); and transferring the encrypted data unit to a target device for decrypting based on information used in the step of generating the differently encrypted data unit (col. 6, lines 4-31).

Claims 41 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Satio as applied to claims 40 and 48 above, and further in view of Ishibaski, US Patent 6,021,199.

As per claim 51, Satio the method of claim 48, wherein the data unit received by the target device is encrypted based on a predetermined encryption key (col. 5, lines 52-56, i.e. the Cmks2= E(ks2, m) encrypted using ks2).

As per claim 54, Satio teaches the method of claim 48, wherein the step of generating the encrypted data unit is performed independently of decrypting the generated encryption unit in the target device (col. 16, lines 14-33).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 41-43, 46 and 49-50, 52-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Satio as applied to claims 40 and 48 above, and further in view of Ishibashi, U.S. Patent 6,021,199 (prior art of record).

As per claims 41 and 49, Satio teaches the method of claim 40. Satio fails to teach but Ishibashi teaches wherein the generated encrypted data unit includes two portions having the

different protection levels spaced apart at a predetermined interval on the data unit (Ishibaski, col. 2, lines 51-60).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the method/system of Satio with the teachings of Ishibaski to generate encrypted data unit which includes two portions having the different protection levels spaced apart at a predetermined interval on the data unit with a motivation to overcome the prior art deficiencies arising from large processing load due to decryption/descrambling of encrypted digital data (Ishibaski, col. 2, lines 1-11).

As per claims 42 and 50, Satio as modified teaches the method of claims 41 and 49 respectively, further comprising the step of storing the generated encrypted data unit in a data storage medium or a digital data player (col. 5, lines 12-16, i.e. the encrypted original data cm0ks1 is transferred to the primary user terminal 4, see also col. 13, lines 61-67).

As per claim 43, Satio teaches the method of claim 41, further comprising the step of decrypting the generated encrypted data unit in the target device (col. 7, lines 54-57).

As per claims 45 and 52, Satio teaches the method of claims 42 and 49 respectively, further comprising the step of reading the generated encrypted data unit from the data storage medium or the digital data player and reproducing the data unit at the request of a user (col. 14, lines 44-53).

As per claim 46, Satio teaches the method of claim 45, further comprising the step of decrypting the data unit based on a predetermined encryption key (col. 14, lines 48-52), and outputting the decrypted data unit to an output line (col. 14, lines 54-61).

As per claim 53, Satio teaches the method of claim 52, further comprising the steps of:

sending the generated encrypted data unit to the digital data player (col. 5, lines 52-56, i.e. the primary user decrypts and reencrypts (i.e. $cmks2=E(ks2, m)$) the data M to store, copy, or transfer to a secondary user terminal 5, col. 6, lines 10-17);

decrypting the generated encrypted data unit based on a predetermined encryption key ; and

outputting the decrypted data unit to an output line of the digital data player (col. 7, lines 54-57, i.e. $M=D(ks2, cmks2)$ using $ks2$ predetermined encryption key, see also (col. 16, lines 7-12 for displaying or editing the data unit in the second terminal, Fig. 5, DISPLAY 49, or STORAGE 51).

7. **Claim 47** is rejected under 35 U.S.C. 103(a) as being unpatentable over Satio and Ishibaski as applied to claim 41 above, and further in view of US patent 6,330,675 Wiser et al. (hereinafter “Wiser”).

Satio as modified teaches the method of claim 41 except wherein the predetermined interval is a multiple or divisor of a buffer size.

However, Wiser teaches system and method for secure transfer of digital data to a local recordable storage medium wherein a digital file is partially encrypted based on a predetermined interval multiple or divisor of a buffer size (Wiser, col. 3, lie 60 through col. 4, line 14, and col. 6, lines 25-34).

Therefore, It would have been obvious to one of ordinary skill in the art to employ the teachings of Wiser in the method/system of Satio as modified to partially encrypt the data unit of Satio based on a predetermined interval multiple or divisor of buffer size to prevent buffer underrun errors (Wiser, col. 6, lines 25-34, see also col. 5, lines 45-60).

Allowable Subject Matter

8. Claims 28-29,31-33, 36 and 38 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. Prior arts made of record, not relied upon:

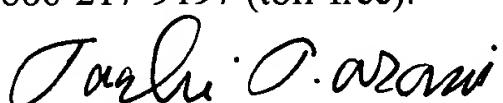
US patent 6,367,019 to Ansell et al.

US patent 5,999,622 to Yaukawa et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Taghi T. Arani, Ph.D.

Examiner

Art Unit 2131

